Institutional trustworthiness and national security governance: Evidence from six European countries

Ball, K., Degli Esposti, S., Dibb, S., Pavone, V. & Santiago-Gomez, E.

Original citation & hyperlink:
Ball, K, Degli Esposti, S, Dibb, S, Pavone, V & Santiago-Gomez, E 2019, 'Institutional trustworthiness and national security governance: Evidence from six European countries', Governance: An International Journal of Policy Administration and Institutions, vol. 32, no. 1, pp. 103-121
https://dx.doi.org/10.1111/gove.12353

DOI 10.1111/gove.12353
ISSN 0952-1895
ESSN 1468-0491

Publisher: Wiley

This is the peer reviewed version of the following article: Ball, K, Degli Esposti, S, Dibb, S, Pavone, V & Santiago-Gomez, E 2018, 'Institutional trustworthiness and national security governance: Evidence from six European countries' Governance, vol. 32 (1), pp. 103-121, which has been published in final form at https://onlinelibrary.wiley.com/doi/epdf/10.1111/gove.12353
This article may be used for non-commercial purposes in accordance with Wiley Terms and Conditions for Self-Archiving.

Institutional Trustworthiness and National Security Governance: Evidence from six European countries

Kirstie Ball*, Sara Degli-Esposti^, Sally Dibb^, Vincenzo Pavone[a], Elvira Santiago-Gomez[o]

* School of Management, University of St Andrews, The Gateway, North Haugh, St Andrews KY16 9RJ, Fife, Scotland
^ Centre for Business in Society, Faculty of Business and Law, Jaguar Building, Coventry University, COVENTRY, CV1 5DL (UK)
[a] Institute of Public Goods and Policies (IPP), Spanish National Research Council (CSIC), c\ Albasanz 26, Madrid (Spain)
[o] Faculty of Sociology, University of Coruña, La Coruña (Spain)

Abstract

This paper examines the relationship between the institutional trustworthiness of security agencies in the context of data intensive security practices. It focuses on the public's acceptance of the way digital surveillance technologies feed into large scale security data analytics. Using the case of Deep Packet Inspection (DPI), survey data gathered in six European countries (n=1,202) demonstrates that security agencies' institutional trustworthiness directly and indirectly influences public acceptance of DPI. Against a backdrop of declining public trust in government and a climate of intense international terrorist threat, governments around the world are appealing to citizens to trade privacy for enhanced security. This paper supports calls for security agencies and their respective governments to engage with the democratic process in order to enrich security and privacy at all levels of public security governance and for the common good.

Institutional Trustworthiness and National Security Governance: Evidence from six European countries

1. Introduction

Surveillance oriented security technologies, or 'SOSTs' (Pavone & Degli Esposti, 2012), are deployed by governments around the world to counter crime and terrorism. SOSTs rely on the use of electronic devices, information infrastructures and data processing capacity to collect and analyze electronic data concerning *inter alia* the communications, financial transactions and travel movements of citizens in order to determine likely threats (Ball, Canhoto et al., 2015). This paper shows that the institutional trustworthiness of security agencies which deploy SOSTs mediates their public acceptance. Examples of SOSTs include smart CCTV, biometric identification systems, location tracking systems, passenger name record sharing and digital communications surveillance technologies.

SOSTs help security agencies safeguard citizens' and national security. Security is part of the common good: without a secure society it would be difficult to run education, health and economic systems, and democratic rights could not be easily exercised (Loader & Walker, 2007). Yet, questions have emerged about these surveillance intensive methods and their potential to undermine the very fabric of the societies that security agencies are there to protect. Questions concern, for example, the levels of privacy intrusion which are associated with SOSTs and the accountability of the security agencies using them.

The paper examines perceptions of one particular SOST, Deep Packet Inspection (DPI). DPI is used by security agencies and internet service providers (ISPs) around the world to read and track the content of internet communications and to filter all web

communications to identify potential targets. It represents a form of "unprecedented and invasive ISP surveillance" (Ohm, 2009, p. 1417) that works by inserting a middle-man, or a gatekeeper, between internet users and those with whom they communicate (Cooper, 2011). DPI is clearly problematic for electronic communications privacy as it enables the content of messages which have not been encrypted to be read by third parties such as security agencies and businesses. Even if the message is encrypted, DPI can still glean information from the messages metadata[i] pertaining to the sender, the receiver and their activities.

The theoretical approach that is used combines perspectives from risk analysis, public administration and organizational psychology to examine the institutional trustworthiness of security agencies in the context of DPI. It draws on survey data gathered at nine citizen consultation events held in six European countries in 2014 (n=1,202). The day-long events, called 'Citizen Summits', required citizens to evaluate DPI in their own national contexts. The deliberative research method chosen ensured that study participants had time to familiarize themselves with a complex technology such as DPI and reflect on its risks and benefits. Trustworthiness was measured through a composite score that accounted for its three internal dimensions: competence, benevolence and integrity (Mayer, Davis et al., 1995).

This paper provides evidence as to the strong direct effect of perceived institutional trustworthiness on the public acceptance of DPI. Institutional trustworthiness also influences perceptions of DPI's effectiveness, which then contributes to an increase in its public acceptance. The results also confirm those of previous studies, which address the mediating role of technology risks and benefits on their public acceptance (Bronfman & Vázquez, 2011). When DPI is perceived to be operated by trustworthy security agencies, the public are more inclined to believe that it is effective and hence

more willing to accept it as a legitimate security solution. They are also more inclined to consider that the technology is less intrusive and again be more willing to accept it. Second, however, when DPI is believed to be operated by untrustworthy security agencies, the more that the public perceive it to be intrusive, the more critical they become and the less likely they are to believe in its effectiveness and support its use. Furthermore, the findings suggest that the more citizens consider security agencies to be competent, honest and to be acting in the public interest, the more likely they are to support the use of DPI.

These results do not imply, however, that security agencies need to pursue a charm offensive in order to carry out intrusive mass surveillance. Instead, the paper contributes to the ongoing debate within public administration scholarship about the merits of enhanced participation between citizens and public policing and security agencies as part of the common good (Tyler & Fagan, 2008; Robinson, Liu et al., 2013; Williams, 2015). The paper acknowledges skepticism about the adoption of transparent and accountable measures by security agencies, with claims that disclosing confidential information may jeopardize national security (Colaresi, 2014). In this sense, it has been argued that security delimits what democratic mechanisms may achieve, by placing certain aspects of security practice beyond democratic scrutiny (Huysmans, 2014).

The paper counters these arguments by drawing on the work of Loader and Walker (2007) who propose an agenda for developing security as a 'thick' public good. They call for the state to engage in four processes. First, the open consideration of resource distribution between security agencies; second, clarity as to the security stakeholders and their interests so that they be effectively regulated, for example, through the licensing of security providers; third, the placing of fundamental rights at the heart of security policies; and finally, the public deliberation and contestation of security

priorities. These ideas inform a research agenda explored in the final sections of the paper which draws on the deliberative turn recently witnessed in public administration research and practice. Specifically, it proposes that research may focus on the mechanisms which foster trustworthiness between the public and those institutions which are charged with protecting national security and hold the latter to account.

2. The security context

2.1 Internet surveillance using deep packet inspection

Deep Packet Inspection (DPI) is used by security agencies and internet service providers around the world to read and track the content of internet communications and to filter all web communications to identify potential targets. DPI takes place in routers, computers which direct traffic around the internet. When a message is sent, it is broken down into smaller chunks called 'packets'. Each packet has several layers, which contains different information about the message: a header, referred to as 'metadata' in legislation and the media, which is the address of the packet; and a payload, its contents. Internet service providers need to inspect some of the message's packets for it to be delivered. In most cases, it is only necessary to review metadata to enable delivery. DPI, however, involves looking beyond the headers to inspect all packets of a message including the payloads. In delivering oral evidence to the U.K. government's Intelligence and Security Committee in 2013, BAE Systems Detica, which supplies DPI to the British Government, described it as a flexible technology which "…gives you the ability to look at what is going on the network and make decisions about what you want to do with what's travelling on the network" (ISC, 2013, p. 20).

DPI is acknowledged as a growing area in the development of both commercial and security applications (Research&Markets, 2017). It was originally developed to detect

malware, but is now also used to manage digital rights, target advertising and identify malicious, dangerous or criminal activity online, such as the distribution of child pornography, hate speech or terrorism (Wehner, 2013). National security agencies around the world can perform DPI by either routing commercial information flows through their own infrastructures (Clement, 2013), or by tapping those of information services providers (Campbell, 2016). British security agencies use DPI to as a means to access communications data from uncooperative overseas Communications Service Providers (ISC, 2013). It was implicated in the Snowden revelations and features in the NSA and GCHQ's shared Upstream and Tempora programs (Porcedda, 2013). The NSA routinely filters huge swathes of web communications using DPI at suspected filtering centers all over North America, alongside AT&T/Fairview surveillance centers in Europe and the U.S.[ii]. As well as mass surveillance, DPI has been linked to online censorship by politically repressive regimes, with allegations it was used by the Libyan and Egyptian government to crush dissent in the Arab Spring (Fuchs, 2013). In 2016, Procera Networks witnessed an internal crisis over its decision to sell DPI technology in Turkey, particularly over whether to fulfil their client's request to be able extract personal passwords from unencrypted data streams (Lauterbach, 2017).

European laws severely restrict the use of DPI for commercial purposes. British Telecom, Virgin Media and Talk Talk fell foul of these laws in 2008 when their service 'Phorm' relied on DPI. Phorm allowed ISPs to track their customers' internet use to personalize advertising on the web pages they subsequently visit for advertising purposes (Bernal, 2011). The controversy emerged in 2008 when it was revealed that BT had secretly run trials on tens of thousands of customers without their consent (Williams, 2008). As a result, the European Commission referred the U.K. to the European Court of Justice for breaching E.U. data protection rules (EDRi, 2010). By

contrast in the U.S., where it is unregulated, the commercial uses of DPI are booming (Wehner, 2013).[iii]

The use of DPI by security agencies therefore potentially benefits society by identifying the perpetrators of serious offences and, by consequence, reducing victimization. However, there are direct privacy harms associated with its use as well as harms to the rights which are qualified by privacy, such as freedom of speech. The prospect of having one's communications read by a government agency produces a chilling effect (Askin, 1972). Such concerns are emphasized when its use by repressive regimes to quell dissent and censor online content are considered. Furthermore, because the identities of those agencies who use DPI, their purposes and its location are opaque in all instances, it is difficult to hold accountable. For citizens, therefore, its appropriate use is a matter of how trustworthy they perceive security agencies to be.

2.2 Trustworthiness and security governance

Studies in the field of public administration have revealed that the institutional trustworthiness of government bodies depends on public perceptions of their performance and the quality of the democracy they engender (Cleary & Stokes, 2006). Evidence from South Korea suggests that public trust in national government can be enhanced by initiatives addressing performance, transparency, citizen participation and the exercise of democratic rights (Kim & Lee, 2012). In Europe and the US, local initiatives designed to repair trust and stimulate political participation such as e-government (Tolbert & Mossberger, 2006), ethics regulation (Cowell, Downe et al., 2014) and participatory decision making (Cooper, Knotts et al., 2008), have met with some success; but trust in national government remains low. Low trust in government is

interpreted as a barometer of dissatisfaction with government programs, party polarizations and economic change, among other things (Kim, 2010).

There is evidence from public opinion surveys that public trust in government is particularly sensitive to government actions around national security matters. For example, in 2001, trust in the United States federal government briefly increased with its muscular response to 9/11 but then decreased the following year (Tolbert & Mossberger, 2006). The picture, however, varies according to the type of security agency in question. Across Europe citizens appear to trust the police significantly more than they do the legal or the political system and, with the exception of Greece, Czech Republic, Slovakia, Poland, Slovenia, Denmark and the Netherlands, citizens trust the police more than they do each other (Ortiz-Ospina & Roser, 2017). At the E.U. level, citizens who trust the European Union tend to be more in favor of E.U. wide security measures than those who do not (EC, 2017). Overall, however, in the last ten years there has been a systematic decline of public trust in government in both Europe and the U.S. (Levi & Stoker, 2000; Tolbert & Mossberger, 2006).

The picture is made more complex by the fact that security governance extends beyond the boundaries of the public sector. National security provision is now distributed across a wide range of private security providers, as well as government agencies. Private security providers include those which supply physical security services, technical advice and training in various military contexts as well as the large defense contractors who install software and systems (for example, Raytheon, BAE Systems, Qinetiq, and Lockheed Martin). The growth of the private security industry is attributed, in no small degree, to state fiscal crises, the under-resourcing of police forces, the rise of a neoliberal mentality which seeks to make non-state actors responsible for security,

coupled with public worries about crime and terror fueled by the media (Goold, Loader et al., 2010).

Indeed, there is an enduring tension between the public good of maintaining security and private sector interests of profit-making. Adam White (2012) outlines a dialectical relationship between these competing interests, arguing that firms need to internalize more public-spirited security values. There are clear dangers associated with the use of private security contractors where this has not occurred as they are not publicly accountable for their actions (Baker & Pattison, 2012). As the governance systems surrounding national security have already been criticized as unaccountable, ineffective and opaque (Anderson, 2015), this paper argues that any future research agenda will need to take account of the complex inter-organizational relationships which comprise contemporary security practices. Therefore, whilst the primary focus of the empirical work featured concerns security agencies, the paper recognizes that the debate does not end there.

3. Theoretical development and hypotheses

This section outlines the variables which feature in the research design. Public acceptance of DPI is the dependent variable. Independent variables are the institutional trustworthiness of the security agencies which use DPI, and the perceived effectiveness and perceived intrusiveness of DPI.

3.1 Public acceptance of DPI

Acceptance, the dependent variable, combines measures of support for, and resistance to, the use of DPI. Acceptance is the preferred construct in both policy documents and the academic literature (Siegrist, 2008; EC, 2012). Although widely used, it is never

defined. Many authors use the wording “To what extent do you find acceptable the following technology for..?” in their questions, leaving the concept unexplained (Bronfman & Vázquez, 2011). A technology gains public acceptance when it is received favorably or with approval. Consequently, the technology can be used over time without enduring harm and in the knowledge that it conforms to approved standards. Users do not engage in any form of collective, or individual, action which may create disruption to the deployment and implementation of the technology by complaining, protesting, refusing to use the solution or opposing it. Opposition is, therefore, the corollary of acceptance.

A key assumption is that the public will be prepared to use a technology that gains public acceptance, or have it used on their behalf. Consequently, technology adoption becomes a proxy for acceptance. In the case of genetically modified organisms (GMOs), for example, individuals who considered their development and use acceptable were more willing to buy GMO foods than those who did not (Siegrist, 2008). However, as SOSTs are used by security agencies, it is almost impossible to find an action taken by citizens that equates to technological adoption as a proxy for acceptance. Citizens subject to SOSTs rarely have a say on their design and adoption, producing an asymmetry of power between citizens and public authorities. Instead, the extent to which the public support the use of SOSTs by security agencies is the measure adopted in this paper.

To develop the concept, measures are added concerning the public resistance and public avoidance of SOSTS. Insights are drawn from marketing (Lee, Motion et al., 2009), and innovation studies that investigate resistance to, and the avoidance of, new products, brands or innovations (Kleijnen, Lee et al., 2009)[iv]. As such, three dimensions of public acceptance of SOSTs are proposed: *support*, *avoidance* and *resistance*. From this

perspective, public acceptance of SOSTs becomes a multi-item attitudinal measure designed to capture participants' support for SOSTs, as well as their concerns and opposition. The resulting indicator is expected to be inversely related to the perceived privacy risk in interacting with SOSTs and directly related to the perceived security benefits.

Public acceptance is distinct from public acceptability. Public acceptability represents a future-oriented concept which help to judge the appropriateness, or legitimacy, of a technology. A technology is acceptable when it has the *potential* of being endured, because it is tolerable, adequate and conforms to approved societal or ethical standards (Degli Esposti, Pavone et al., 2017). By contrast, public acceptance is a past-oriented concept used to assess the extent to which an already adopted technology has triggered public opposition or acceptance. Although acceptance and acceptability are interrelated, public acceptance does not necessarily imply acceptability from a legal or human rights perspective. SOSTs may enjoy high public acceptance but still run contrary to human rights, national constitutional principles, or regulation. Sometimes public acceptance can be the result of repression, lack of freedom of expression or simple inertia or lack of information. Nonetheless, technologies which are considered *acceptable* by the public may well also be technologies *accepted* by the public, depending on when the question is asked.

3.2 Institutional trustworthiness

Trustworthiness is defined as a set of beliefs about a third party that facilitates 'a willingness to depend on [that] party in a situation of risk' (Akter, D'Ambra et al., 2011, p. 100). As SOSTs are deployed to counter threats, they reflect the risks inherent in their context of deployment. SOSTs also create civil liberties risks. If better national security

does not result from the sharing of data—as was the case in Belgium where information sharing did not prevent ISIS attacks—the public legitimacy and trustworthiness of the relevant security agencies suffers (Brunsden, Chassany et al., 2016). Some observers have suggested that traditional intelligence services, such as agent infiltration, would have been more effective in monitoring and tracking down terrorists (Vitali, 2015). Institutional trustworthiness, then, appears that it may be central to the public acceptability of SOSTs.

Trustworthiness can be distinguished from trust in two ways. First, trustworthiness relates to a willingness to act, whereas trust relates to an action which has taken place. As such, trustworthiness reflects beliefs about whether a third party can be relied upon and influences willingness to rely on that party in the future (Colquitt, Scott et al., 2007). Trustworthiness therefore relates to citizen beliefs about the properties of the institution and how they serve their interests. Second, while trust is only experienced at an interpersonal level, trustworthiness can be experienced between individuals and other social entities, such as institutions. Accordingly, institutional trustworthiness is primarily conceptualized as an individual's willingness to trust in what the institution does and stands for, rather than in the people who work within it (Cook & Gronke, 2005).

Three literatures approach trustworthiness with the aim of stabilizing definitions and measurements of the concept: risk analysis, public administration and organizational psychology. Risk analysis advances a 'deficit model' of trustworthiness, arguing that its basis is an institution's superior knowledge of the particular risk with which they are dealing (White & Eiser, 2005). According to the deficit model, citizens lack knowledge and must rely on institutions to address risks for them (Siegrist & Cvetkovich, 2000). Examples include studies of nuclear waste disposal sites (Freudenburg, 1993), food risk

(Eiser, Miles et al., 2002), and other environmental risks (Flynn, Slovic et al., 1994). Workplace studies of trustworthiness also establish that as a consequence of increased institutional trustworthiness, individuals' willingness to accept risk is increased (Mayer, Davis et al., 1995).

Trustworthiness is conventionally measured using an overall trustworthiness measure and several sub-scales. Progress towards a multi-dimensional measure beyond that used in the deficit model has been made in the fields of public administration and organizational psychology, with significant cross fertilization between the two. Research in public administration tends to investigate the trustworthiness of local and national governments (Levi & Stoker, 2000; Tolbert & Mossberger, 2006; Cooper, Knotts et al., 2008; Kim & Lee, 2012), while in organizational psychology the focus is on top management (Schoorman, Mayer et al., 2007). These literatures have established that trustworthiness has at least three principal components.

- *Competence*—whether the institution is perceived to be able to deliver its objectives
- *Benevolence*—whether the institution is perceived to be concerned about the welfare and integrity of the community, as opposed to acting out of self-interest
- *Integrity*—whether the institution is perceived to act in an ethical way and not to abuse its power.

These components have been widely applied, including in relation to the acceptability of mobile-health information systems (Akter, D'Ambra et al., 2011) and e-government (Avgerou, Ganzaroli et al., 2009; Smith, 2011). Reflecting different dimensions of the institution, there is evidence that each component has a separate relationship with overall trustworthiness (Colquitt, Scott et al., 2007). However, the pattern of these

relationships has yet to be clearly established. We now move on to discuss the remaining variables in the research design.

3.3 DPI perceived intrusiveness and effectiveness

All SOSTs bring both security benefits and privacy risks. With the exception of a study by Sanquist, Mahy, and Morris (2008), which investigates security experts' assessments of twelve homeland security solutions[v], the internal dimensions of security benefits and privacy risks remain unexplored. According to this study, solutions were considered more acceptable when they were perceived to improve national security, when participants benefitted from them personally, and when they were seen as a valid response to the security problem they were deployed to solve. These solutions were also considered to pose the lowest threat to civil liberties.

Two factors underpinned participants' responses: the perceived intrusiveness (privacy risks) and the perceived effectiveness (security benefit) of the security solutions. Perceived effectiveness, which was an overall perception of how worthwhile a particular security measure might be, was positively correlated with acceptance. Effectiveness encompassed both perceptions of technical performance (e.g., national security benefit, accuracy) and more general acceptability-oriented attributes (i.e., equitability, transparency, control). Intrusiveness, which concerned the risks of civil liberties infringement, general intrusiveness, embarrassment, financial loss, unauthorized disclosure, and false identification, was negatively correlated with acceptance. In this case, acceptance apparently involved a balance of benefits (SOST perceived effectiveness) and risks (SOST perceived intrusiveness) which are inversely related.

4. Empirical model and corresponding hypotheses

The theoretical model sets out the hypothesized relationships between the perceived trustworthiness of security agencies and public acceptance of SOSTs, controlling for the effect of perceived intrusiveness and effectiveness on acceptance. The relationship between security agencies trustworthiness and SOST intrusiveness and effectiveness is also investigated. The model suggests that the more that citizens perceive DPI to be effective, the more likely they are to accept it (H2a); while the more that citizens perceive DPI to be intrusive, the less likely they are to accept it (H3a); and the less likely they are to find it effective (H3b). Moreover, the more that citizens perceive security agencies to be trustworthy, the more likely they are to accept DPI (H1a); to rate DPI as effective (H1b); and the less likely they are to rate DPI as intrusive (H1c). Finally, public effectiveness (M1 and M3) is expected to mediate the effect of trustworthiness and intrusiveness on acceptance; and public intrusiveness (M2) is expected to mediate the effect of trustworthiness on acceptance. The hypotheses are summarized in figure three.

The following hypotheses relating to citizens' risk assessments and the use of DPI are formulated:

H1a The more that citizens perceive security agencies to be trustworthy, the more likely they are to find DPI acceptable.

The relationship between institutional trustworthiness and citizens' subjective assessments of the risks and benefits of SOST's is also assessed (Siegrist, 2000):

H1b The more that citizens perceive security agencies to be trustworthy, the more likely they are to rate DPI as effective.

H1c The more that citizens perceive security agencies to be trustworthy, the less likely they are to rate DPI as intrusive.

The relationships between effectiveness, intrusiveness and acceptability are tested as follows:

H2a The more that citizens perceive DPI to be effective, the more likely they are to find it acceptable.

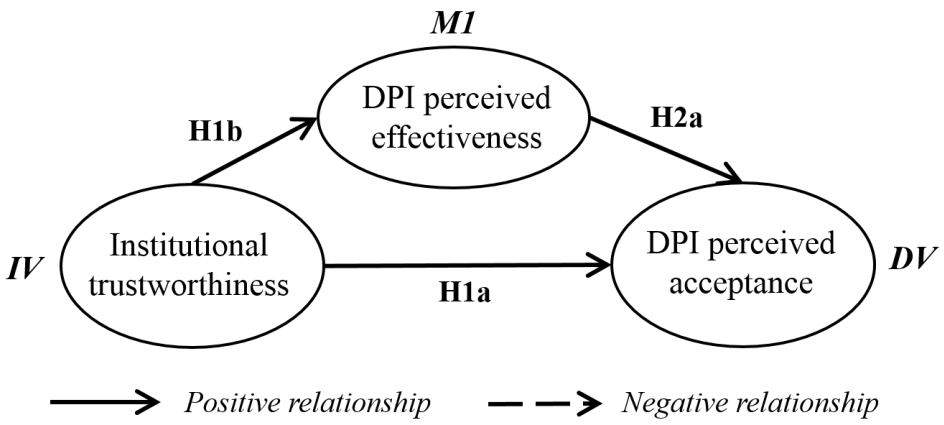
H3a The more that citizens perceive DPI to be intrusive, the less likely they are to find it acceptable.

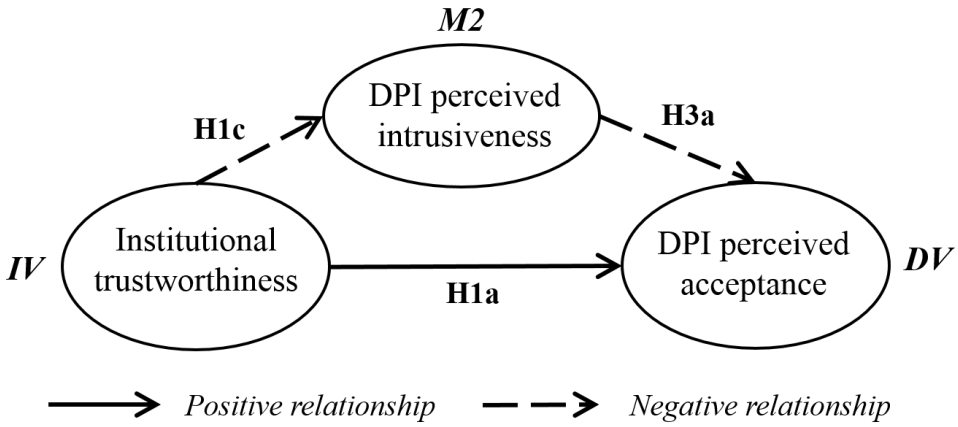
The following mediating effects of citizens' perceptions of intrusiveness and effectiveness on trustworthiness, described in figure one, are tested:

M1: DPI perceived effectiveness will mediate the effect of security agencies' trustworthiness on public acceptance of DPI.

M2: DPI perceived intrusiveness will mediate the effect of security agencies' trustworthiness on public acceptance of DPI.

Figure 1. Mediation effects number one and two





Reflecting the balance of benefits and risks, the following relationship and mediating effect, described in figure two, are tested:

H3b The more that citizens perceive DPI to be intrusive, the less likely they are to find it effective.

M3: DPI perceived effectiveness will mediate the effect of DPI perceived intrusiveness on public acceptance of SOST.

Figure 2. Mediation effect number three

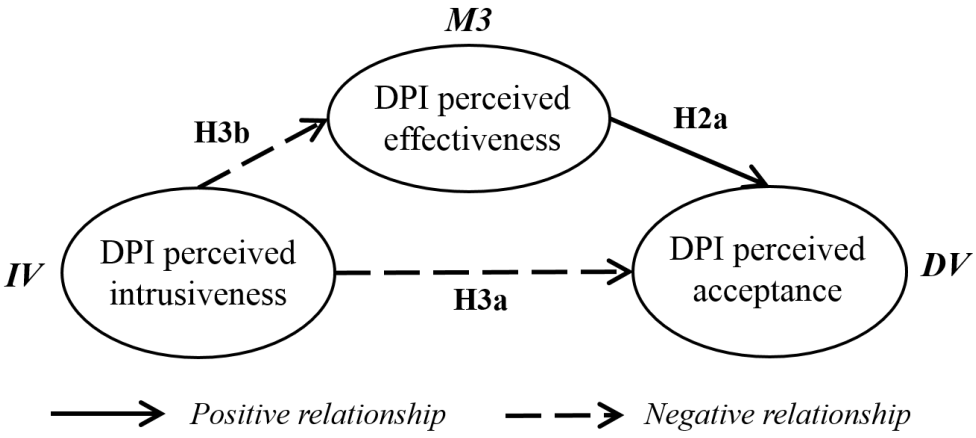
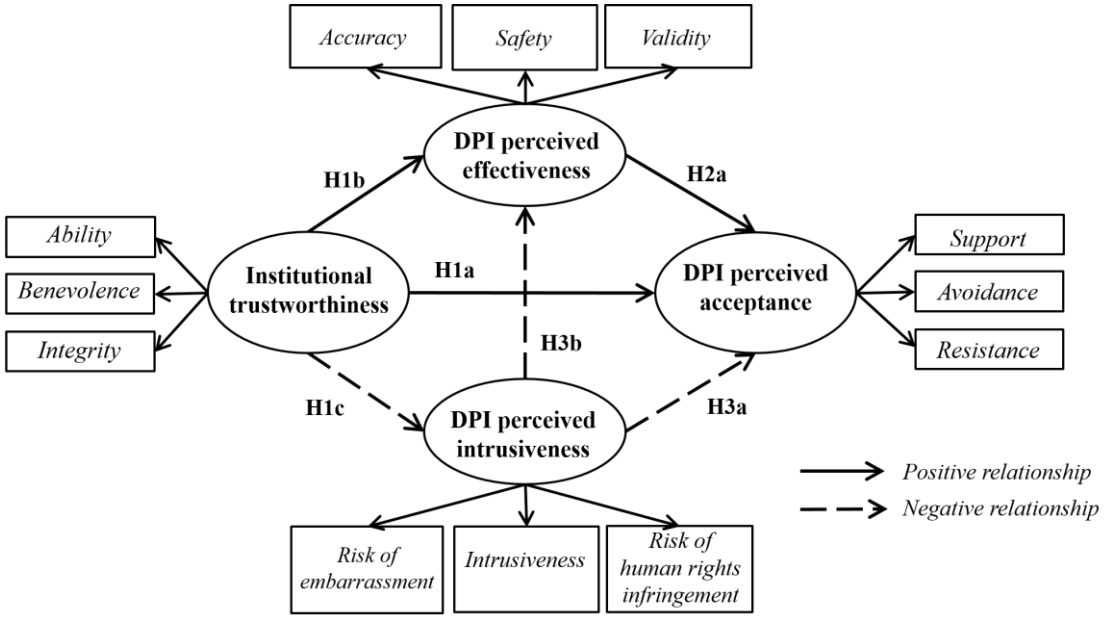


Figure 3. Overall theoretical model



5. Case, method and measurements

Data were drawn from nine citizen summits held in six European countries in the spring of 2014. Citizen summits are a form of public engagement exercise, which have proved effective in raising awareness and increasing democratic participation in matters of political and social importance (Bedsted et al., 2015). The summit design applied combined a participatory ethos with academically rigorous data collection methods. Following previous studies (Grimmelikhuijsen et al., 2013), countries were grouped into clusters using Hofstede's (2003) criteria to ensure that DPI was considered across a spread of national cultures. Countries were clustered where their scores were similar along a majority of Hofstede's five dimensions: power-distance, individualism, masculinity, uncertainty avoidance and long-term orientation. The clusters represented North Europe (Norway and U.K.), Central (Austria and Switzerland) and Southern Europe (Italy and Spain). Two hundred citizens attended each summit and participants were recruited against national demographic profiles. It is important to note that the

results are not generalizable to country level but do represent some interesting points of comparison. Details of the sample are given in table one.

Table 1. Study participants' characteristics

Country	No. of study participants	Female	Younger than 50 years old	Children (<16) at home	Belonging to a minority ethnic group
1. Austria	234	51%	51%	18%	21%
2. Italy	191	53%	50%	21%	26%
3. Norway	129	54%	47%	33%	12%
4. Spain	180	47%	66%	21%	10%
5. United Kingdom	214	47%	61%	39%	26%
6. Switzerland	254	58%	41%	30%	38%
Total	*1,202*				

Each summit considered two SOSTs, of which DPI was one. The research design ensured that participants were familiar with the use, functions, benefits and limits of DPI before making their assessments. Prior to attending the event, participants received an information magazine which explained the issues under discussion and the benefits and risks associated with DPI and other SOSTs[vi]. This information was supplemented with a seven-minute documentary film shown during the summits[vii]. The films and the magazine were produced by the research team. The materials were read and absorbed by the majority of the participants. They were asked whether they understood what DPI was before the discussions started. With the exception of the U.K., the majority said they agreed or strongly agreed with the statement "I understand what DPI is" (Austria: 65%; Italy: 53%; Norway: 74%; Spain: 60%; U.K.: 31%; Switzerland: 75%). The large majority of study participants in each country also agreed or strongly agreed with the statement "I have gained new insight by participating in the citizen summit" (Austria 72%; Italy 93%; Norway 89%; Spain 77%; U.K. 90%; Switzerland 85%).

At each summit, participants sat in table groups. There were approximately 25 discussion groups per summit, each comprising around eight participants, a note-taker

and a facilitator. The day-long events were divided into segments in which participants viewed one of the documentary films, discussed the content in their table groups and then answered questions in plenary about their views. During the table discussions the facilitators ensured that the participants were able to identify the national security agencies to which the discussion related. Plenary questions were answered using an audience response system, with participants using a voting handset to record their responses on a five-point Likert scale.

Significant effort was deployed during questionnaire development to ensure that it was effective for use in a plenary voting setting. Questions had to be short and simple, with clear wording which avoided double negatives. Multi item measures for single subscales felt repetitive and so a careful choice of measures had to be made. Reversing scales within question batches were avoided, as they caused confusion. Questions had to be built in a logical order, so that the head facilitator could enliven them for the participants. Immediate feedback was given to the participants so that they could see the spread of responses in the room and feel more engaged in the process. The measures used are shown in table two.

Table 2. Constructs' dimensions and questionnaire items

DPI perceived acceptance (DV)	
Construct dimension	*Questionnaire item*
1. DPI Support	"Overall I support the adoption of DPI as a national security measure." (5-points Likert scale)
2. DPI Avoidance	"Please choose the statement you mostly agree with: 1. I would not go online because of DPI 2. I would avoid going online because of DPI 3. I do not think I would change my behavior online 4. I would change how I behave online because of DPI **5.** I would definitely not change my behavior online."
3. Opposition to DPI	"Please choose the statement you mostly agree with: 1. I am prepared to use any means I can to prevent its use 2. I am prepared to campaign actively against its use 3. I would support others who were protesting against its use 4. I would like to find out more how to protect my privacy **5.** I do not oppose it at all."

DPI perceived effectiveness (IV)	
Construct dimension	*Questionnaire item*
4. Accuracy	"In my opinion, DPI is an effective national security tool." (5-points Likert scale)
5. Safety	"When I am online, I feel more secure because DPI is used." (5-points Likert scale)
6. Validity	"DPI is an appropriate way to address national security threats." (5-points Likert scale)
DPI perceived intrusiveness (IV)	
Construct dimension	*Questionnaire item*
7. Risk of embarrassment	"The idea of DPI makes me feel uncomfortable." (5-points Likert scale)
8. Perceived intrusiveness	"I feel DPI is forced upon me without my permission." (5-points Likert scale)
9. Risk of human rights infringement	"DPI worries me because it could violate my fundamental human rights." (5-points Likert scale)
Institutional trustworthiness (IV)	
Construct dimension	*Questionnaire item*
10. Ability	"Security agencies which use DPI are competent at what they do." (5-points Likert scale)
11. Benevolence	"Security agencies which use DPI are concerned about the welfare of citizens as well as national security." (5-points Likert scale)
12. Integrity	"Security agencies which use DPI do not abuse their power." (5-points Likert scale)

Participants engaged with the risks, benefits and use contexts of DPI. Its benefits were that it could improve information security and the fight against crime by identifying and blocking harmful or criminal messages. Participants were told that it could prevent cybercrime by preventing the spread of computer viruses and assist in the detection of crime and provide evidence in an investigation. The risks were that it removed communications privacy, had a chilling effect on democratic debate, was relatively unregulated, the users of it were difficult to hold to account, and it was not always effective at detecting illegal material. Table three gives the descriptive statistics for each variable.

Table 3. Descriptive statistics for all variables in the model

n = 1,202	*Mean*	*Std. Dev.*	*Skewness*	*Kurtosis*
DPI perceived acceptance				
1. Overall I support the adoption of DPI as a national security measure	2.87	1.47	-0.35	-1.00
2. Active avoidance of DPI	3.41	1.41	-1.18	0.86
3. Challenging the use of DPI for security purposes	3.05	1.54	-0.84	-0.59
DPI perceived effectiveness				
4. In my opinion, DPI is an effective national security tool	2.91	1.42	-0.41	-0.75
5. When I am online, I feel more secure because DPI is used	2.02	1.18	0.35	-0.52
6. DPI is an appropriate way to address national security threats	2.84	1.42	-0.38	-0.75
DPI perceived intrusiveness				
7. I feel DPI is forced upon me without my permission	4.14	1.44	-1.89	2.56
8. The idea of DPI makes me feel uncomfortable	3.58	1.45	-0.97	0.07
9. DPI worries me because it could violate my fundamental human rights	3.92	1.46	-1.49	1.25
Institutional trustworthiness				
10. Security agencies which use DPI are competent at what they do	2.49	1.38	-0.43	-0.75
11. Security agencies which use DPI are concerned about the welfare of citizens as well as national security	2.64	1.39	-0.35	-0.80
12. Security agencies which use DPI do not abuse their power	2.08	1.26	0.13	-0.73

6. Findings

Evidence was found to support all hypotheses and the presence of three partial mediation effects, which are reported in table four. The results confirm that increased institutional trustworthiness increases public acceptance of DPI (H1a: p=0.32**)[viii]. Institutional trustworthiness is also a key antecedent of how citizens evaluate security benefits and privacy impacts. Establishing institutional trustworthiness in the context of DPI also increases public perceptions of SOST effectiveness (H1b: p=0.53**) and decreases SOST perceived intrusiveness (H1c: p=-0.27**). DPI effectiveness was

shown to have a strong direct effect on public acceptance (H2a: p=0.56**); it also partially mediates the relationship between trustworthiness and public acceptance (M1: p=0.35**). As such, where there are high levels of institutional trustworthiness, the public are likely to interpret DPI as effective. Similarly, where there are high levels of institutional trustworthiness, the public is likely to interpret DPI as less intrusive (H1c: p=-0.27**). However, high levels of perceived DPI intrusiveness was shown to reduce both SOST acceptance (H3a: p=-0.19) and SOST perceived effectiveness (H3b: p=-0.21**) and to partially mediate the relationship between institutional trustworthiness and public acceptance of DPI (M2: p=0.60**). Finally, effectiveness partially mediates the effect of intrusiveness on acceptance (M3: p=-0.21**).

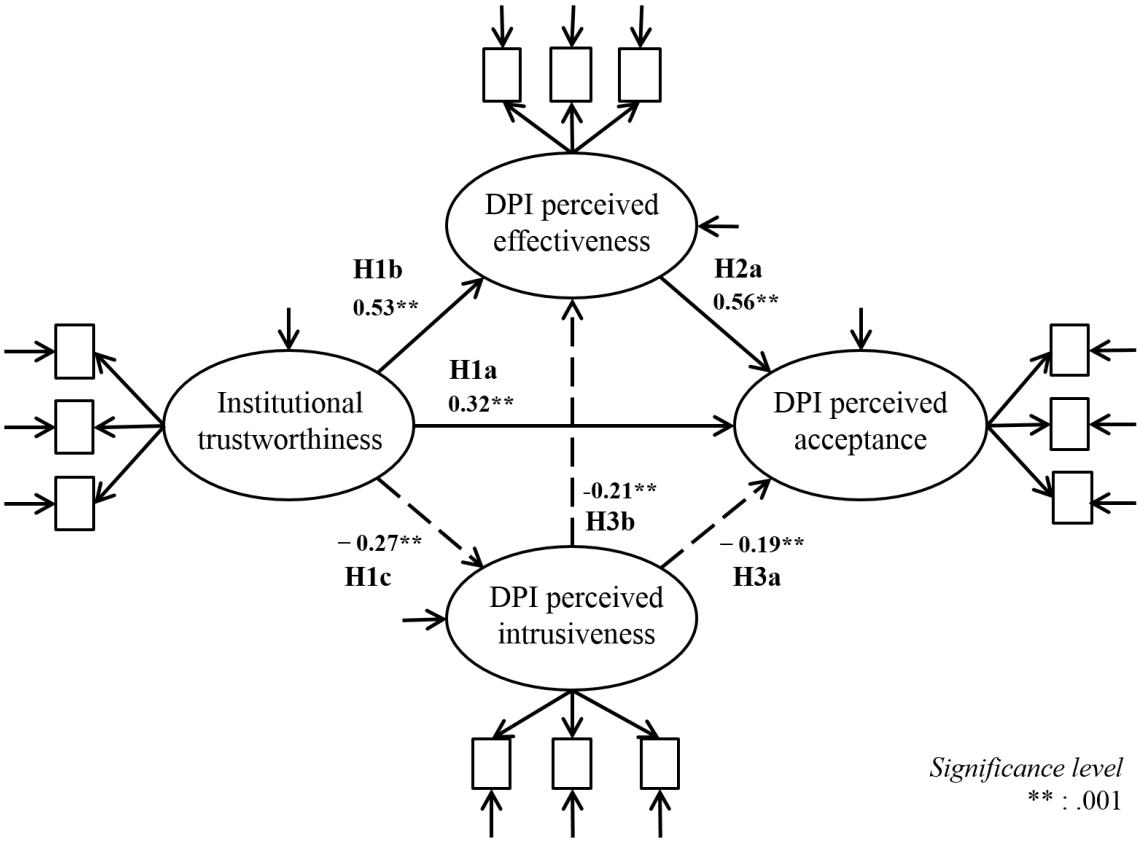
Table 4. Tested mediation effects

	IV => M => DV	Direct effect without mediator	Direct effect with mediator	Indirect effect	Outcome
M1	TRU => EFF => ACC	0.737 (Sig. .001)	0.351 (Sig. .001)	Sig. .004	Partial mediation effect
M2	TRU => INT => ACC	0.737 (Sig. .001)	0.603 (Sig. .001)	Sig. .004	Partial mediation effect
M3	INT => EFF => ACC	-0.492 (Sig. .001)	-0.210 (Sig. .001)	Sig. .005	Partial mediation effect

Figure four presents an overview of the results. In brief, the more security agencies are perceived to be trustworthy when handling DPI, the more positive the participants were about its use (H1a). Those who perceive security agencies to be trustworthy are also more likely to consider DPI as an effective security measure (H1b) and support its use (H2a). In contrast, those who consider DPI intrusive are more critical and more willing to question its effectiveness as a security measure (H3b). Furthermore, the less people perceive security operators to be trustworthy, the more likely they are to consider DPI as an intrusive measure (H1c) and unwilling to accept its use (H3a). Both intrusiveness (M2) and effectiveness (M1) have an influence on the effect that security agents' perceived trustworthiness exercise on people's willingness to accept DPI. Finally,

perceiving DPI as an effective measure decreases people's concerns about its intrusiveness, which in turn contributes to increase DPI acceptance (M3).

Figure 4. Overall empirical model



Hypotheses were tested using structural equation modelling—SEM (Bowen & Guo, 2011), and the Asymptotic Distribution Free estimator (Browne, 1984), which does not require data to be normally distributed (Ding, Velicer et al., 1995). The model was tested on a total sample of 1,202 usable cases. Sample size satisfied the condition for the correct use of large-sample estimation methods, which requires a ratio of observed variables over sample size larger than 1:50. Measurement reliability was assessed by computing Louis Guttman's (1945) split-half reliability coefficient. Cronbach's (1951) Alpha reliability coefficient was used to estimate a scale's internal consistency (Sheng & Sheng, 2012). Results of these tests show good levels of reliability (Lance, Butts et al., 2006) for all constructs (trustworthiness: Alpha 0.74; Split-half: 0.73; effectiveness:

Alpha 0.70; Split-half: 0.71; intrusiveness: Alpha 0.57; Split-half: 0.47), and acceptable levels for the dependent variable (acceptance: Alpha 0.56; Split-half 0.51). All other model fit indexes show very good results (CFI = .949; GFI = .979; RMSA = .029). Computed bias-corrected confidence intervals (95% confidence level; 2,000 bootstrap samples) were calculated to assess the presence of mediation effects by adopting Andrew Hayes' (2013) approach and Reuben Baron and David Kenny's (1986) procedure.

7. Trustworthiness and the public acceptance of DPI: Towards a research agenda

The results demonstrate that the perceived trustworthiness of security agencies shaped participants' evaluations of the effectiveness, intrusiveness and thence their acceptance of DPI. This finding is significant for a number of reasons. First, it confirms Dourish and Anderson's (2006), view that the institutional context is critical in shaping participants' perceptions about the acceptability, perceived effectiveness and intrusiveness of SOSTs. Second, the identified mediation effects highlight that this institutional shaping is powerful and pivotal, in that it impacted the participants' perceptions in both positive and negative ways. Low trustworthiness was associated with increased perceptions of intrusiveness and high trustworthiness with increased perceptions of effectiveness. Third, the negative effect exercised by the perceived intrusiveness of DPI on its perceived effectiveness appears at first to support the view that these two variables are inversely related, reinforcing notions that enhancing both security and privacy is difficult to achieve (Monahan, 2006; Tsoukala, 2006). However, while security and privacy have been presented in the media and by policymakers as incompatible, we argue that this incompatibility is not a foregone conclusion. As there

is a clear institutional dimension shaping these perceptions, we argue that there may be measures and mechanisms which meaningfully and substantively address citizens' concerns about intrusiveness so that security benefits and privacy protections are both maximized. A society whose public institutions protect fundamental rights is experienced as much more secure than one which does not.

Indeed, there is public policy value in seeking to protect both privacy and security. It has been suggested, for instance, that privacy should be integrated into, rather than pitched against, security policy (Solove, 2011); and that excessive surveillance undermines, rather than enhances, security (Landau, 2011). These stakes rise if the data are subsumed into opaque security practices driven by data analytics, as is the case with DPI. Security measures could be assessed in relation to their overall impact on all security assets present in a society (Pavone, Santiago Gomez et al., 2016). How then may this be achieved in practice? The public experience of security rests as much on the deployment of armed forces overseas as it does in neighbourhoods and high streets, implicating many layers of governance. Democratic due process is key to fostering trustworthiness in national security governance arrangements and states must take strong responsibility for governing diverse security stakeholders in a democratically robust and transparent way (Loader and Walker, 2007). However, fostering trustworthiness is not a simple matter, as it has three dimensions—benevolence, competence and integrity—which need to be considered and, as these results show, are relevant to public perceptions (Mayer, Davis et al., 1995).

Reflecting competence, the first question concerns whether the state should set up regulatory arrangements which monitor and disseminate the consequences of resource distribution in security. National standards of service could be devised to govern diverse security providers. These standards would need to go beyond profit seeking and serve

the interests of the broader community. Public reporting on security agency performance directly relates to public perceptions of their competence in addressing threats. Reflecting benevolence, the second question concerns the extent to which the state should seek to determine whether different sections of society who are subject to different security risks are experiencing appropriate levels of security and receiving appropriate protection. Furthermore, the state needs to understand how security protections intersect with other forms of social protection for vulnerable groups. To what extent can the state devise and maintain mechanisms of conversation and contestation so that different points of view may be recognized and constructively incorporated into policy? Citizen participation in security agendas hence relates to perceptions of benevolence: that the agency is acting in the interests of the whole community. Reflecting integrity, rights are a vital ingredient of national security and the state must ensure that there are appropriate mechanisms for ensuring that human rights are incorporated into security enactments. Efforts to improve transparency and to encourage exercise of democratic rights in security settings will influence perceptions of integrity: whether the agency will 'do the right thing' and not abuse its power.

These suggestions, which are based on Loader and Walker's (2007) analysis, inform the development of a research agenda in this area. They imply that the democratic process can be used to embrace differences of opinion in relation to security matters at a number of levels, rather than silence them, as Huysmans (2014) has warned. Attention is particularly drawn to whether the deliberative turn, recently emerged in other areas of public administration, may be mobilized in relation to security governance in a substantial and meaningful way. In Latin America, for example, the potential for the democratization of state-society relations has been famously tested through 'participatory budgeting' (Avritzer, 2009), whilst in Europe innovative mechanisms like

‘Citizens Juries’, ‘Citizens Panels’ and ‘Open Space’ have become more common (Fung, 2003). More recently such innovations have been supplemented by mechanisms that are realized through new digital technologies, such as electronic voting, ‘hackathons’, ‘living labs’, ‘maker spaces’ and online discussion forums (Webster & Leleux, 2018). Future research may assess whether any of these and other mechanisms could be mobilized in the security sphere, and the levels, practices and institutions in which they could be so mobilized.

Furthermore, mobilising the democratic process goes beyond merely inviting citizens to engage with such mechanisms. As Arnstein (1969) has famously highlighted, the labelling of citizen-state interaction as ‘participatory’ can in fact result in the marginalization of certain voices and an overwhelming pressure to comply with and consent to whatever the state wishes to accomplish. Research needs to address how citizens may see themselves as having a voice and being able to contribute meaningfully in security settings. If citizens have been subject to discriminatory state practices in the past, they may well find such participation challenging. Research may also examine the impact of citizen attempts to empower themselves in the face of security institutions, so that they may develop their capacity to question the security to which they are subject. Research also needs to determine which outcomes of deliberative processes would be most meaningful in terms of enhancing institutional trustworthiness so that citizens can see for themselves how their participation has had an impact. Participatory spaces are populated with policy professionals whose expertise will necessarily constitute what they can and cannot say in these settings, as well as the arguments that they support or oppose. If strongly entrenched political actors are controlling the participation, what are the opportunities for change? How may the boundaries of these institutions be made more porous? Research may examine the points in the security governance structure

which are the most amenable to deliberation and engagement, including intersections with third party providers and private sector organizations. It may also examine how local arrangements can facilitate citizens and consumers being informed, consulted, involved in or co-producers of the means and ends of security. The method deployed in this paper—citizen summits, where security solutions are deliberated by the general public—provides a template for action.

The paper also makes a number of methodological contributions. First, it confirms that the approach to the measurement of trustworthiness adopted in public administration and organizational psychology can be applied in national security settings. In this approach, institutional trustworthiness is a composite measure incorporating three subscales. A closer look at the sub-components of institutional trustworthiness also confirms significant relationships with each of the public acceptance measures. This finding indicates that no single subcomponent was dominant, and that no one feature of the security agencies was outstanding in terms of its influence. Competence, benevolence and integrity were all strongly related to overall acceptance (Kendall's Tau nonparametric association test: p=.275**; .341**; .278** respectively). As benevolence showed a slightly stronger correlation, the paper recommends that further research should examine whether participants sought particular assurance that security agencies were working for the benefit of all in society. Second, it advances new multi-scalar measures of public acceptance, improves on the single item measures used in previous research. Third, it consolidates the suggestions made by Sanquist, Mahy, and Morris (2008) that both effectiveness and intrusiveness are underpinned by a series of subcomponents. Accuracy, perceived safety and validity underpin effectiveness and consent, discomfort and risk of human rights infringement underpin intrusiveness.

DPI is a highly intrusive technology, uppermost in the public's mind at the time the fieldwork was undertaken because of the then recent Snowden revelations. It is pertinent to question whether these findings can be generalized for all other SOSTs. Analysis of data collected about other SOSTs which took place during the fieldwork—smart CCTV and smartphone location tracking—may confirm these findings. Unfortunately, space limitations prevent a description and investigation of each case in the current paper. Nevertheless, the methodology presented would enable this study to be repeated in other settings.

8. Conclusion

This paper is the first to examine the institutional trustworthiness of security agencies in the current surveillance-intensive climate. It explored public views about internet surveillance undertaken by national security agencies by means of Deep Packet Inspection (DPI). It drew on survey data gathered at nine citizen consultation events held in six European countries in 2014. The findings suggested that the perceived trustworthiness of security agencies positively influences perceptions of the effectiveness of DPI and its overall acceptance. The more trustworthy the security agencies were perceived to be, the more likely DPI was considered as an effective and appropriate security intervention and the less likely it was perceived as intrusive. The findings support calls for security agencies and their respective governments to engage with transparency and the democratic process in order enrich both security and privacy at all levels of public security governance and for the common good. If trustworthiness is significant for an intrusive surveillance method such as DPI, the likelihood of its importance for other intrusive surveillant security methods cannot and should not be ignored. These results suggest that an opportunity exists for security agencies to enrich

both security and privacy by adopting policies and practices which foster trustworthiness in practice and in the eyes of the public.

References

Akter, S., D'Ambra, J., & Ray, P. (2011). Trustworthiness in mHealth information services: An assessment of a hierarchical model with mediating and moderating effects using partial least squares (PLS). *Journal of the American Society for Information Science and Technology*, *62*(1), 100-116.

Anderson, D. (2015). A question of trust: Report of the investigatory powers review. *Independent Reviewer of Terrorism Legislation*. Retrieved 14/10/2016, from https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf

Arnstein, S. R. (1969). A ladder of citizen participation. *Journal of the American Institute of Planners*, *35*(4), 216-224.

Askin, F. (1972). Surveillance: The social science perspective. *Columbia Human Rights Law Review*, 4, 59-88.

Avgerou, C., Ganzaroli, A., Poulymenakou, A., & Reinhard, N. (2009). Interpreting the trustworthiness of government mediated by information and communication technology: lessons from electronic voting in Brazil. *Information Technology for Development*, *15*(2): 133-148.

Avritzer, L. (2009). *Democracy and the Public Space in Latin America*. Princeton, NJ: Princeton University Press.

Baker, D. P., & Pattison, J. (2012). The principled case for employing private military and security companies in interventions for human rights purposes. *Journal of Applied Philosophy*, *29*(1), 1-18.

Ball, K., Canhoto, A. I., Daniel, E., Dibb, S., Meadows, M., Ball, K., & Spiller, K. (2015). *The Private Security State?: Surveillance, Consumer Data and the War on Terror*. Copenhagen, Denmark: Copenhagen Business School Press.

Baron, R. M., & Kenny, D. A. (1986). The moderator–mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. *Journal of Personality and Social Psychology*, *51*(6): 1173.

Bedsted, B., Gram, S., Joergensen, M. J., & Kluver, L. (2015). WWViews on biodiversity: New methodological developments and ambitions. In M. Rask and R. Worthington (Eds.), *Governing Biodiversity Through Democratic Deliberation* (pp. 27-40). New York, NY: Routledge.

Bernal, P. (2011). *Rise and Phall: lessons from the phorm saga*. In S. Gutwirth, Y. Poullet, P. De Hert and R. Leenes, *Computers, Privacy and Data Protection: An Element of Choice* (pp. 269-283). Dordrecht, The Netherlands: Springer.

Bowen, N. K., & Guo, S. (2011). *Structural Equation Modeling*. Oxford, UK: Oxford University Press.

Bronfman, N. C., & Vázquez, E. L. (2011). A cross-cultural study of perceived benefit versus risk as mediators in the trust-acceptance relationship. *Risk Analysis: An International Journal*, *31*(12), 1919-1934.

Browne, M. W. (1984). Asymptotically distribution-free methods for the analysis of covariance structures. *British Journal of Mathematical and Statistical Psychology*, *37*(1), 62-83.

Brunsden, J., Chassany, A.-S., & Jones, S. (2016). Europe's failure to share intelligence hampers terror fight. Retrieved 14/10/2016, from https://www.ft.com/content/f9baf7e8-f975-11e5-b3f6-11d5706b613b

Campbell, D. (2016). Big Brother is born, and we find out 15 years too late to stop him. Retrieved 11/04/2018, from http://www.theregister.co.uk/2015/12/16/big_brother_born_ntac_gchq_mi5_mass_surveillance_data_slurping

Cleary, M. R., & Stokes, S. C. (2006). *Democracy and the Culture of Skepticism: Political Trust in Argentina and Mexico*. New York, NY: Russell Sage Foundation.

Clement, A. (2013). "IXmaps—Tracking your personal data through the NSA's warrantless wiretapping sites". Paper presented at the 2013 IEEE International Symposium on Technology and Society (ISTAS): Social Implications of Wearable Computing and Augmediated Reality in Everyday Life, 27-29 June 2013, Toronto, Canada.

Colaresi, M. P. (2014). *Democracy Declassified: The Secrecy Dilemma in National Security*. Oxford, UK: Oxford University Press.

Colquitt, J. A., Scott, B. A., & LePine, J. A. (2007). Trust, trustworthiness, and trust propensity: A meta-analytic test of their unique relationships with risk taking and job performance. *Journal of Applied Psychology*, *92*(4), 909-927.

Cook, T. E., & Gronke, P. (2005). The skeptical American: Revisiting the meanings of trust in government and confidence in institutions. *Journal of Politics*, *67*(3), 784-803.

Cooper, A. (2011). Doing the DPI Dance. In W. Aspray and P. Doty (Eds.), *Privacy in America: Interdisciplinary Perspectives* (pp. 139-165). Lanham, MD: Scarecrow Press.

Cooper, C. A., Knotts, H. G., & Brennan, K. M. (2008). The importance of trust in government for public administration: The case of Zoning. *Public Administration Review, 68*(3), 459-468.

Cowell, R., Downe, J., & Morgan, K. (2014). Managing politics? Ethics regulation and conflicting conceptions of "good conduct". *Public Administration Review*, *74*(1), 29-38.

Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika*, *16*(3), 297-334.

Degli Esposti, S., Pavone, V., & Santiago-Gomez, E. (2017). Aligning security and privacy: The case of Deep Packet Inspection. In R. Bellanova, J. Čas, J. P. Burgess, M. Friedewald and W. Peissl, *Surveillance, Privacy and Security: Citizens' Perspectives* (pp. 71-90). London, UK: Routledge.

Ding, L., Velicer, W. F., & Harlow, L. L. (1995). Effects of estimation methods, number of indicators per factor, and improper solutions on structural equation modeling fit indices. *Structural Equation Modeling: A Multidisciplinary Journal*, *2*(2), 119-143.

Dourish, P., & Anderson, K. (2006). Collective information practice: emploring privacy and security as social and cultural phenomena. *Human-Computer Interaction*, *21*(3), 319-342.

EC (2012). *Action Plan for an Innovative and Competitive Security Industry*. COM(2012) 417 final. Brusells, Belgium: European Commission.

EC (2017). Standard Eurobarometer 87: Spring 2017 first results. *Public opinion in the European Union Series*. Retrieved 11/04/2018, from http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/STANDARD/surveyKy/2142

EDRi (2010). The Phorm case sends the UK to the European Court Of Justice. Published on 6th October. Retrieved 11/04/2018, from https://edri.org/edrigramnumber8-19uk-infringement-data-protection/

Eiser, J. R., Miles, S., & Frewer, L. J. (2002). Trust, perceived risk, and attitudes toward food technologies. *Journal of Applied Social Psychology*, *32*(11), 2423-2433.

Flynn, J., Slovic, P. & Mertz, C. K. (1994). Gender, race, and perception of environmental health risks. *Risk Analysis*, *14*(6), 1101-1108.

Freudenburg, W. R. (1993). Risk and recreancy: Weber, the division of labor, and the rationality of risk perceptions. *Social Forces*, *71*(4), 909-932.

Fuchs, C. (2013). Societal and ideological impacts of Deep Packet Inspection. *Information, Communication and Society*, *16*(8), 1328-1359.

Fung, A. (2003). Deliberative Democracy, Chicago Style: Grass-roots Governance in Policing and Public Education. In A. Fung & E. O. Wright (Eds.), *Deepening democracy: Institutional innovations in empowered participatory governance* (pp. 111-143). London: Verso.

Goold, B., Loader, I., & Thumala, A. (2010). Consuming security? Tools for a sociology of security consumption. *Theoretical Criminology*, *14*(1), 3-30.

Grimmelikhuijsen, S., Porumbescu, G., Hong, B., & Im, T. (2013). The effect of transparency on trust in government: A cross-national comparative experiment. *Public Administration Review*, *73*(4), 575-586.

Guttman, L. (1945). A basis for analyzing test-retest reliability. *Psychometrika*, *10*(4): 255-282.

Hayes, A. F. (2013). *Introduction to Mediation, Moderation, and Conditional Process Analysis: A Regression-Based Approach*. New York, NY: The Guilford Press.

Hofstede, G. (2003). *Culture's Consequences: Comparing Values, Behaviors, Institutions and Organizations across Nations*. New York, NY: Sage Publications.

Huysmans, J. (2014). *Security Unbound: Enacting Democratic Limits*. London, UK: Routledge.

ISC (2013). Oral evidence—BAE Systems Detica, 17 October 2012. Access to communications data by the intelligence and security Agencies. *Presented to Parliament by the Prime Minister by Command of Her Majesty.* February. Retrieved 19/02/2018, from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/225120/isc-access-communications.pdf

Kim, S. (2010). Public trust in government in Japan and South Korea: Does the rise of critical citizens matter? *Public Administration Review, 70*(5), 801-810.

Kim, S., & Lee, J. (2012). E-participation, transparency, and trust in local government. *Public Administration Review, 72*(6), 819-828.

Kleijnen, M., Lee, N., & Wetzels, M. (2009). An exploration of consumer resistance to innovation and its antecedents. *Journal of Economic Psychology, 30*(3), 344-357.

Lance, C. E., Butts, M. M., & Michels, L. C. (2006). The sources of four commonly reported cutoff criteria: What did they really say? *Organizational Research Methods, 9*(2), 202-220.

Landau, S. (2011). *Surveillance or Security?: The Risks Posed by New Wiretapping Technologies*. Cambridge, MA: MIT Press.

Lauterbach, C. (2017). No-go zones: Ethical geographies of the surveillance industry. *Surveillance & Society*, *15*(3/4), 557-566.

Lee, M. S., Motion, J., & Conroy, D. (2009). Anti-consumption and brand avoidance. *Journal of Business Research*, *62*(2): 169-180.

Levi, M., & Stoker, L. (2000). Political trust and trustworthiness. *Annual Review of Political Science*, *3*(1): 475-507.

Loader, I., & Walker, N. (2007). *Civilizing security*. Cambridge, MA: Cambridge University Press.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review*, *20*(3), 709-734.

Monahan, T. (2006). *Surveillance and Security: Technological Politics and Power in Everyday Life*. New York, NY: Taylor & Francis.

Ohm, P. (2009). The rise and fall of invasive ISP surveillance. *University of Illinois Law Review*, 1417-1496.

Ortiz-Ospina, E., & Roser, M. (2017). Trust. *Our World in Data*. Retrieved 11/04/2018, from https://ourworldindata.org/trust

Pavone, V., & Degli Esposti, S. (2012). Public assessment of new surveillance-oriented security technologies: Beyond the trade-off between privacy and security. *Public Understanding of Science*, *21*(5), 556-572.

Pavone, V., Santiago-Gomez, E., & Jaquet-Chifelle, D.-O. (2016). A systemic approach to security: Beyond the tradeoff between security and liberty. *Democracy and Security, 12*(4), 225-246.

Porcedda, M. G. (2013). Lessons from PRISM and Tempora: the self-contradictory nature of the fight against cyberspace crimes. Deep packet inspection as a case study. *Neue Kriminalpolitik, 25*(4), 373-389.

Research&Markets (2017). Deep Packet Inspection (DPI)—Global Strategic Business Report. Retrieved 11/03/2018, from https://www.researchandmarkets.com/research/bwx2jv/deep_packet

Robinson, S. E., Liu, X., Stoutenborough, J. W., & Vedlitz, A. (2013). Explaining popular trust in the Department of Homeland Security. *Journal of Public Administration Research and Theory*, *23*(3), 713-733.

Sanquist, T. F., Mahy, H., & Morris, F. (2008). An exploratory risk perception study of attitudes toward homeland security systems. *Risk Analysis: An International Journal*, *28*(4), 1125-1133.

Schoorman, F. D., Mayer, R. C., & Davis, J. H. (2007). An integrative model of organizational trust: Past, present, and future. *Academy of Management Review*, *32*(2), 344-354.

Sheng, Y., & Sheng, Z. (2012). Is coefficient alpha robust to non-normal data? *Frontiers in Psychology*, *3*(34), 1-13.

Siegrist, M. (2000). The influence of trust and perceptions of risks and benefits on the acceptance of gene technology. *Risk Analysis: An International Journal*, *20*(2), 195-204.

Siegrist, M. (2008). Factors influencing public acceptance of innovative food technologies and products. *Trends in Food Science & Technology*, *19*, 603-608.

Siegrist, M., & Cvetkovich, G. (2000). Perception of hazards: The role of social trust and knowledge. *Risk Analysis*, *20*(5), 713-720.

Smith, M. L. (2011). Limitations to building institutional trustworthiness through e-government: a comparative study of two e-services in Chile. *Journal of Information Technology*, *26*(1), 78-93.

Solove, D. J. (2011). *Nothing to hide: The false tradeoff between privacy and security*. New Haven, CT: Yale University Press.

Tolbert, C. J., & Mossberger, K. (2006). The effects of e-government on trust and confidence in government. *Public Administration Review*, *66*(3), 354-369.

Tsoukala, A. (2006). Democracy in the light of security: British and French political discourses on domestic counter-terrorism policies. *Political Studies*, *54*(3), 607-627.

Tyler, T. R., & Fagan, J. (2008). Legitimacy and cooperation: Why do people help the police fight crime in their communities. *Ohio State Journal of Criminal Law*, *6*, 231.

Vitali, F. (2015). Comunicazione e controllo ai tempi del terrore." *LIMES*, 11, 141-146.

Webster, C. W. R., & Leleux, C. (2018). Smart Governance: Opportunities for technologically-mediated citizen co-production. Information Polity, 1-16.

Wehner, C. (2013). Deep Packet Inspection—Use Cases, Requirements and Architectures. Retrieved 14/10/2016, from http://www.eetimes.com/document.asp?doc_id=1280856

White, A. (2012). The new political economy of private security. *Theoretical Criminology, 16*(1), 85-101.

White, M. P., & Eiser, J. R. (2005). Information specificity and hazard risk potential as moderators of trust asymmetry. *Risk Analysis, 25*(5), 1187-1198.

Williams, C. (2008). BT pimped customer web data to advertisers last summer: Denied secret relationship with Phorm, blamed malware. Published on 27 Feb 2008 at 13:29, Retrieved 11/03/2018, from http://www.theregister.co.uk/2008/02/27/bt_phorm_121media_summer_2007/

Williams, L. M. (2015). Beyond enforcement: Welcomeness, local law enforcement, and immigrants. *Public Administration Review, 75*(3), 433-442.

Notes

[i] Metadata are data about data. They can include information about when a document was created, and what changes have been made on that document. In the case of internet activity, metadata give information on IP addresses of senders and recipients of emails, volume of data uploaded or downloaded, time and duration of web connection, location data, and so on.

[ii] See IXmaps, an internet mapping tool developed by the University of Toronto which provides information on internet routing and associated privacy and security issues. IXmaps is available at https://www.ixmaps.ca/

[iii] Worldwide there are currently just under 30 providers of DPI to ISPs and governments, including the following: Allot Communications Ltd. (Israel); Bivio Networks, Inc. (Canada); Cisco Systems, Inc. (U.S.); cPacket Networks, Inc. (U.S.); Huawei Technologies Co., Ltd. (China); Procera Networks (U.S.); Qosmos (France); R&S Cybersecurity ipoque GmbH (Germany); Sandvine Incorporated ULC (Canada); SolarWinds Worldwide, LLC (U.S.); SonicWALL L.L.C. (U.S.) and Vedicis (U.S.) (Research&Markets 2017).

[iv] In drawing on these literatures we acknowledge that resistance is a core concept in the sociological canon, based on deep, historical descriptions of the social world using a variety of data sources. As a phenomenon with a strong basis in praxis, the concept's dimensions have not been easily quantifiable and scales not readily derived.

[v] Airport passenger and baggage screening; explosive detector canines; hidden camera surveillance of individuals for gait analysis and facial recognition; data mining of individual business and financial transactions; passports with RFID tags; monitoring of Internet and email; location tracking through global positioning systems in cell phones and cars; travel tracking through Secure Flight and other risk assessment systems; trusted traveller programs to speed up security screening; national identity card; citizen observers; radiation monitoring at border crossings.

[vi] The magazine and an overview of the films can be found at: http://surprise-project.eu/wp-content/uploads/2014/04/SurPRISE-D4.3-Information-material-and-documentary-films.pdf

[vii] The films can be viewed at: http://surprise-project.eu/dissemination/information-material-from-the-participatory-events/

[viii] ** denotes a confidence interval of 99%.